REMARKS

Claims 1-29 were pending and presented for examination and in this application. In an Office Action mailed May 16, 2007, claims 1-29 were rejected. Applicant thanks Examiner for examination of the claims pending in this application and addresses Examiner's comments below.

Applicants are amending claim 14 in this Amendment and Response to correct a typographical error.

The specification was objected to because of informalities. Applicants have amended paragraphs 0017 and 0033 of the specification to address these informalities. No new matter has been added by this amendment.

Applicants' representative conducted a telephone interview with Examiner San Juan and his supervisor on August 9, 2007, in order to discuss claim 18 and the cited references. A summary of the interview is incorporated into these Remarks as part of the discussion of claim 18. Applicants thank the Examiners for their time and remarks.

In view of the telephone interview and the Remarks that follow herein, Applicants respectfully request that the Examiner reconsider all outstanding objections and rejections, and withdraw them.

Response to Rejection Under 35 USC 102(b) in View of Roberts and Hickman

Claims 1-29 stand rejected under 35 USC §102(b) as allegedly being anticipated by U.S. Patent No. 6,295,551 ("Roberts") and by U.S. Patent No. 6,173,332 ("Hickman"). Applicants respectfully traverse the Examiner's rejections of the pending claims.

Because the interview of August 9th centered on claim 18, Applicants address it first, and then proceed to address the other independent claims. Independent claim 18 recites, in relevant part (emphasis added):

> A method of sharing data across a computing system, the method comprising:
> subsequent to an initial authentication of a user, receiving requests to authenticate the authenticated user from a plurality of applications on a plurality of computing platforms being accessed by the authenticated user;
> automatically authenticating the authenticated user to the plurality of applications being accessed by the authenticated user *responsive to the initial authentication of the user*;
> ...

Thus, claim 18 recites receiving requests to authenticate the authenticated user *subsequent to an initial authentication*, and automatically authenticating the authenticated user *responsive to the initial authentication*.

Applicants' representative discussed claim 18 in a telephone interview on August 9, 2007, focusing specifically on the second limitation. At the conclusion of the interview, the Examiner's supervisor stated that the Roberts and Hickman references did not appear to show the limitation, and that as a result the rejection would likely be withdrawn and another search performed. Logic supporting this conclusion follows.

The first cited reference, Roberts, discusses a call center system enabling a call center representative and a calling party to jointly browse World Wide Web content while simultaneously conducting a voice conversation. (Abstract) After a user provides a password, the server provides an applet enabling the joint activities (11:5-44). Specifically, the server provides a user applet to the calling party's computer and a service applet to the call center representative's computer (Abstract). The applets then can proceed to share data

(16:9-39), such as a demonstration or form. After initial authentication of each user, data is exchanged, with no need for subsequent authentication of the users.

Roberts does not disclose, teach, or suggest "subsequent to an initial authentication of a user, receiving requests to authenticate the authenticated user from a plurality of applications on a plurality of computing platforms being accessed by the authenticated user." In column 11, lines 14-15 (cited by the Examiner), and the surrounding text, Roberts explains that a password system is part of ascertaining and validating which type of user (e.g., calling party or call center representative) is logging in, and thus which type of applet the server should transmit. Lines 14-15 merely reveal that other users can join a current session merely by also logging in using the same username / password validation codes. There is no suggestion that the other users have been *initially authenticated*; rather, since the validation codes referenced in the cited portion are used for initial login, this passage instead suggests that the users have *not* been initially authenticated. Nor is there any suggestion that any such requests come from a *plurality of applications*.

Nor does Roberts disclose, teach, or suggest "automatically authenticating the authenticated user to the plurality of applications being accessed by the authenticated user *responsive to the initial authentication* of the user." Column 11, lines 31-35 (cited by the Examiner) merely discloses that the username / password validation codes determine the type of applet downloaded, so that a given person may choose the desired type of applet by providing the proper related validation codes. Again, there is no suggestion that the user had been *initially authenticated*, and thus there cannot be a subsequent automatic authentication *responsive to* an initial authentication. Nor is there a suggestion that a *plurality of applications* is involved. Further, the Examiner's stated "undergoing the same process as

usually done for the initial authentication" does not in any way constitute *automatic* authentication of the authenticated user, given that the initial authentication involved the requester / user inputting a username and password.

The second cited reference, Hickman, discusses a cluster computer system including multiple network accessible computers that are each coupled to a network, and a method for providing access to host computers by client computers over a computer network. (Abstract) The virtual machine program enabling access by client computers is first set up on the host computer (12:56-13:57), and then the client controls the host machine remotely (14:8-49). After the authentication information needed for access is specified on the host (13:41) and the client user provides the key (14:26-28), information is transmitted between the host and the client, such as screen updates to be displayed on the client screen (13:19-20).

Hickman does not disclose, teach, or suggest "subsequent to an initial authentication of a user, receiving requests to authenticate the authenticated user from a plurality of applications on a plurality of computing platforms being accessed by the authenticated user" and "automatically authenticating the authenticated user to the plurality of applications being accessed by the authenticated user responsive to the initial authentication of the user." Column 13, lines 41-42 and column 14, lines 26-30 (cited by the Examiner) respectively disclose a user providing and the system storing, along with the web address from which the system can be accessed, authentication information, and receiving an encryption / decryption key from the client user at the time that the virtual machine is run. The disclosed encryption merely shows a way to maintain the secrecy of information sent between two endpoints, but does not reveal receiving a request to authenticate the authenticated user from an application. Further, even if it were considered to do so, it would merely relate to the single host / client

endpoint pair, and would fail to show requests from a *plurality of applications* being accessed by the authenticated user, as claimed.

Thus, claim 18 is patentable over both Roberts and Hickman.

Independent claim 1 recites, in relevant part (emphasis added):

> A cross-platform single sign-on system for sharing user data across computers on a plurality of computing platforms, the system comprising:
> an authentication module for authenticating a user at the beginning of a computing session;
> an interface module configured to receive requests for authentication and non-authentication data associated with the user from a plurality of applications on the plurality of computing platforms and, *based upon authentication of the user* at the beginning of the computing session *and responsive to the requests*, to automatically provide authentication and non-authentication data to the plurality of applications throughout the computing session;
> ...

Thus, claim 1 is similar to claim 18, reciting automatically providing authentication data *based upon* authentication of the user at the beginning of the computing session. As noted in the above discussion of claim 18, and stated in the telephone interview with the Examiners, neither Roberts nor Hickman discloses or suggests the similar limitation of automatically authenticating an authenticated user to the plurality of applications being accessed by the authenticated user *responsive to the initial authentication* of the user, and thus both likewise fail to disclose or suggest the limitation at hand.

In particular, Roberts's column 11, lines 5-15, and column 8, lines 18-20 (cited by the Examiner), respectively disclose determining the type of user requesting an applet via a validation system, such as one involving username and password, and that a server, rather than an applet, may transmit shared content (non-authentication data). It is not inherent in this disclosure that authentication data will be

automatically provided to a plurality of applications based upon authentication of the user at the beginning of the computing session; rather, only shared content need be transferred between applets, with no further need for authentication data after initial authentication.

Regarding Hickman, column 21, lines 27-30, and column 19, lines 9-16 (cited by the Examiner), respectively disclose that after username, password, and system requirements are successfully provided, the cluster administration computer has the information required to allow a user access, and that a personal state can include information about the state of the user's operating system. However, neither of these citations in any way discloses or suggests automatically providing authentication data based upon authentication of the user at the beginning of the computing session, as claimed.

Thus, claim 1 is patentable over both Roberts and Hickman for at least the same reasons discussed above with respect to claim 18.

Independent claim 14 recites:

> A data registry for storing and providing data across a computing system, the data registry comprising:
> a plurality of user data entries, each of the user data entries describing a unique user of a computing system comprised of a plurality of computing platforms and a plurality of applications;
> a plurality of authentication entries associated with each of the user data entries for authenticating the user on the plurality of applications of the computing system; and
> a plurality of non-authentication attributes and attribute entries associated with each of the user data entries in which information about a user's use of an application can be preserved.

Thus, claim 14 recites a data registry comprising user data entries, authentication entries, and non-authentication attributes and attribute entries, with

each user data entry having associated with it a plurality of authentication entries and a plurality of non-authentication attributes and attribute entries. As noted in the Specification at paragraphs 0019 and 0029, the data registry represents a single storage location, implemented, for example, by a RDBMS database.

In contrast, Roberts fails to disclose or suggest "a plurality of authentication entries associated with each of the user data entries for authenticating the user on the plurality of applications of the computing system." Even assuming *arguendo* that the Roberts applets constitute "applications," each user data entry of Roberts is associated with exactly one applet type applicable to that user. See Roberts column 10, line 56 to column 11, line 4, in which the sign-on information for a given user determines the applet downloaded. Thus, since each user identity is associated with a single applet, it follows that each user data entry in Roberts at best has only one authentication entry, not a plurality, as claimed. Nor does Roberts disclose the registry comprising a plurality of *non-authentication* attributes about the use of an application. Regarding the cited passages, storing only which applet is associated with a user does not constitute a *plurality* of non-authentication attributes, and there is no suggestion that the cited session box information is stored in the alleged registry—rather, the session box information only displays information about the current session, and thus there would be no reason to store it in the registry.

Regarding Hickman, note that the "personal state" of cited column 21, lines 27-31 must be "located on the Internet" (column 22, line 10) after the login information was provided earlier at column 21, line 15. Thus, since it must be located after the login information is entered and verified, it must be stored separately from

the authentication data, and thus Hickman cannot disclose a data registry comprising both authentication and non-authentication data, as claimed. Further, cited column 22, lines 20-24, and column 22, lines 29-31, disclose that the system will compare various network-accessible computers (NACs) to the user's request in order to find a computer meeting the minimum requirements of the user, but does not disclose a plurality of authentication entries for authenticating the user on the plurality of *applications*, as claimed. Rather, only one authentication entry is needed, since the login is to the computer as a whole, and not to the claimed plurality of applications.

Thus, claim 14 is patentable over both Roberts and Hickman.

Based on the above remarks, Applicants respectfully submit that for at least these reasons claims 1, 14, and 18 are patentably distinguishable over the cited references. Therefore, Applicants respectfully request that Examiner reconsider the rejection, and withdraw it.

All the dependent claims depend, directly or indirectly, from independent claims 1, 14, or 18, and recite additional patentably distinguishable features and limitations. They are therefore allowable for at least the same reasons discussed above with reference to their respective independent claims.

Conclusion

In sum, Applicants respectfully submit that claims 1-29, as presented herein, are patentably distinguishable over the cited references. Therefore, Applicants request reconsideration of the basis for the rejections to these claims and request allowance of them.

In addition, Applicants respectfully invite Examiner to contact Applicants' representative at the number provided below if Examiner believes it will help expedite furtherance of this application.

Respectfully Submitted,
MICHAEL A. HORWITZ, ET AL.

Date: August 16, 2007

By: /Sabra-Anne R. Truesdale/
Sabra-Anne R. Truesdale
Registration No. 55,687
FENWICK & WEST LLP
801 California Street
Mountain View, CA 94041
Phone: (650) 335-7187
Fax: (650) 938-5200
E-Mail: struesdale@fenwick.com